LES PUBLICATIONS

[EN CLAIR]

DRONES ET CYBERSÉCURITE : PRÉVENIR LES ATTAQUES CONTRE LES SYSTÈMES MILITAIRES

Par L. A.-F. & Janelle B.

LES JEUNES IHEDN

À PROPOS DE L'ARTICLE

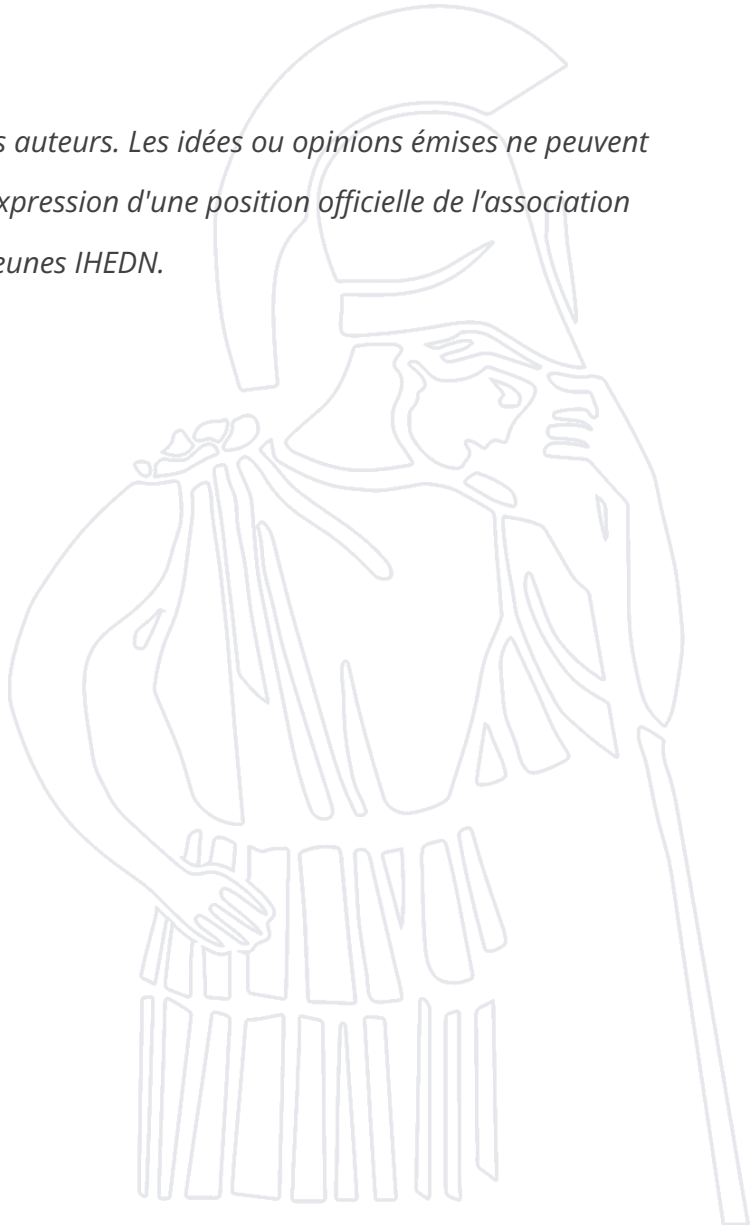
Cet article répertorie les principales cybermenaces auxquelles sont exposés les drones militaires, et les moyens de protection qui y sont associés.

À PROPOS DES AUTEURS

L. A.-F. : Travaillant dans le secteur privé, il est responsable de la Délégation Internationale en Suisse.

Janelle B : Responsable de la Délégation Internationale Allemagne.

Ce texte n'engage que la responsabilité des auteurs. Les idées ou opinions émises ne peuvent en aucun cas être considérées comme l'expression d'une position officielle de l'association Les Jeunes IHEDN.



Un drone, en droit français, est un *« engin mobile terrestre, aérien ou naval, sans équipage embarqué, programmé ou télécommandé et réutilisable. Les drones militaires sont équipés de systèmes d'armes ou de recueil de renseignements »*[1]. Systèmes duaux et sensibles, les drones en tant qu'armes sont aussi victimes de la guerre qui se déroule dans le cyberespace. Dès 2011, un rapport du Sénat rappelle deux épisodes marquants : l'infection par un virus informatique des postes de commande à distance des drones américains *Predator* et *Reaper* par un disque dur externe, et le détournement d'un drone au-dessus de l'Iran la même année[2]. Partant de cette définition et du constat que ces systèmes façonnent désormais les théâtres de guerre contemporains, il convient de lister les cybermenaces qui leur sont associées, en ce qu'elles dépassent désormais les scénarios fictifs créés par les hautes autorités[3]. Nous étudierons ensuite les mécanismes de défense développés pour parer à ces menaces.

État des lieux des menaces

Cette liste n'est pas exhaustive mais couvre une majeure partie des attaques possibles contre les drones militaires, dont certaines sont communes à tous les aéronefs, civils ou militaires (comme les menaces liées à l'utilisation du système GPS). Elle reprend des éléments qui peuvent être catégorisés dans le modèle de menaces sur les systèmes électroniques, « STRIDE »[4].

[1] *Journal Officiel de la République française n° 0141* [en ligne]. texte n° 46, 19 juin 2011, p. 1496 [consulté le 16/03/2025]. Disponible sur : https://www.legifrance.gouv.fr/download/pdf?id=mg2HM0nti9zNAO_Y5gj1ExwZjgCJ5g7nDrxqDEoMGrY=.
[2] « La cyberdéfense : un enjeu mondial, une priorité nationale ». *Sénat* [en ligne], rapport d'information n° 681 (2011-2012), 18 juillet 2012. Disponible sur : https://www.senat.fr/notice-rapport/2011/r11-681-notice.html.
[3] *Cf.* scénario fictif dans : General ALLEN, John R. & HUSAIN Amir. « On Hyperwar ». *U.S Naval Institute* [en ligne], juillet 2017 [consulté le 18/02/2025]. Disponible sur : https://www.usni.org/magazines/proceedings/2017/july/hyperwar.
[4] *Spoofing, Tampering, Repudiability, Information disclosure, Denial of Service, Elevation of Privilege*. Source : CURZI, Simone ; NEVICO, Anthony ; DAVIS, Jonathan ; PAZOS RODRIGUEZ, Rafael & HANSON, Ben. « Integrating threat modeling with DevOps ». *Microsoft* [en ligne], 12 juillet 2022 [consulté le 13/03/2025]. Disponible sur : https://learn.microsoft.com/en-us/security/engineering/threat-modeling-with-dev-ops.

Risques associés aux échanges de données en temps réels

GPS Jamming : Brouillage, réalisé en émettant de puissants signaux qui saturent les fréquences utilisées par le système GPS. Les systèmes sont désorientés et ne peuvent déduire leur position qu'à partir de leurs centrales inertielles (gyroscopes et accéléromètres).

GPS Spoofing : Usurpation et falsification des signaux. Les récepteurs GPS suivent généralement le signal le plus fort disponible. Le signal contrefait ayant une intensité supérieure à celui des satellites authentiques, il les préempte et transmet des données erronées. Cette préemption peut être difficile à détecter si le signal "pirate" copie initialement le signal légitime et dépasse peu à peu son intensité.

Man-in-the-Middle attack : Interception des échanges entre le drone et la station télépilote. Elles peuvent être passives (interception à des fins de renseignement) ou actives (modification ou blocage des communications).

Denial of Service (DoS / DDos) : Afflux de requêtes sur les fréquences de communication avec le drone (*flooding attack*) ou sur les infrastructures terrestres (empêchant l'opération des systèmes de contrôle du drone) entre autres.

Risques associés aux logiciels (*software*)

Backdoors : Dans le cas de logiciels fournis par des entités étrangères, bien que vendus et promis comme étant autonomes, ils peuvent être l'objet de portes dérobées (backdoors) conçues délibérément par le fabricant, pour garder un moyen d'accès difficilement détectable par le client.

Zero-day vulnerabilities : les vulnérabilités "jour-zéro" sont des failles de sécurité inconnues ou pas encore corrigées. Tous les systèmes informatiques y sont sujets.

Risques associés aux composants électroniques (hardware)

Des altérations de composants en amont de la chaîne d'approvisionnement peuvent introduire des failles exploitables à distance (permettant par exemple le contrôle, l'extraction de données ou la destruction sur commande). Une occurrence connue récente est le sabotage avant la livraison de talkies-walkies, par les services secrets israéliens, de bipeurs utilisés par le Hamas[5].

Les possibles mesures de protection et de lutte contre les menaces

Des mécanismes et technologies déjà opérationnels permettent de se prémunir de certaines de ces vulnérabilités.

Les ondes étant le seul moyen pour l'exploitant de communiquer avec son outil, le chiffrement des signaux est indispensable. Celui-ci peut concerner le lien entre le pilote et son drone (contrôle, lien vidéo, etc.) ou les signaux externes qui « alimentent » le drone. Par exemple, le chiffrement des signaux GPS depuis le satellite, (voir le système SAASM états-unien[6]) permet une authentification du signal qui empêche sa falsification et donc le spoofing.

Les avancées technologiques récentes, notamment dans le domaine de l'intelligence artificielle (IA) et plus particulièrement du Machine Learning, ouvrent de nouvelles portes pour la détection et la mitigation d'attaques DoS[7].

[5] SALLON, Hélène. « Explosions de bipeurs au Liban : le Hezbollah pris au piège dans son soutien au Hamas ». *Le Monde* [en ligne], 19 septembre 2024 [consulté le 16/03/2025]. Disponible sur : https://www.lemonde.fr/international/article/2024/09/19/explosions-de-bipeurs-au-liban-le-hezbollah-pris-au-piege-dans-son-soutien-au-hamas_6324066_3210.html.

[6] « What are Selective Availability Anti-Spoofing Modules (SAASM)? ». *EverythingRF* [en ligne], 20 août 2022 [consulté le 13/03/2025]. Disponible sur : https://www.everythingrf.com/community/what-are-selective-availability-anti-spoofing-modules.

[7] ALSUMAYT, Albandari et *all*. « Detecting Denial of Service Attacks (DoS) over the Internet of Drones (IoD) Based on Machine Learning ». *Sci* [en ligne], 2024, 6, 56, 2024. [consulté le 13/03/2025]. Disponible sur : https://doi.org/10.3390/sci6030056.

Ces protections ne doivent pas seulement concerner le système de drone en lui-même ; on l'a vu, un ciblage qui neutraliserait la station télépilote rendrait le drone isolé quand bien même ses systèmes seraient parfaitement opérationnels. Pour cela, d'autres procédures peuvent être mises en place *a posteriori* ; comme la préparation et l'importation dans le drone de plans de secours mis en œuvre en cas de rupture du lien avec le télépilote (pré-chargement des points survolés et actions associées, bascule sur une autre station télépilote, retour autonome à la base…).

Quant à la chaîne de conception et d'approvisionnement, elle doit être sécurisée et idéalement souveraine pour éviter les ingérences ou interactions étrangères qui pourraient être dissimulées.

Nous avons donc listé les principales cybermenaces auxquelles sont sujets les drones militaires, et les moyens de défense qui y sont associés. En tout état de cause, de nombreuses ressources sont dévouées à la protection cyber de ces systèmes, de la phase de conception à la phase d'opération, en passant par les outils externes qui viennent le « nourrir » en données. Toutefois, la course technologique livrée par des acteurs malveillants, à des fins de neutralisation ou de piratage - par exemple pour en faire des vecteurs d'attaque[8] - met en exergue la nécessité de renforcer les investissements en recherche et développement, visant à garantir la sécurité et l'opérabilité de ces outils.

[8] Bureau de Lutte contre le Terrorisme. « Protéger les cibles vulnérables contre les attaques terroristes impliquant des systèmes de drones aériens ». *Un.org* [en ligne]. Disponible sur : https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/2118451f-vt-mod5-unmanned_aircraft_systems_web.pdf.






publication@jeunes-ihedn.org